UNITED STATES DISTRICT COURT

FILED
2008 MAR 28 AM 10: 16
CLERK US DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA
DEPUTY

SOUTHERN DISTRICT OF CALIFORNIA

In the Matter of the Search of
(Name, address or brief description of person or property to be searched)

1097 Emerald Ave,
El Cajon, California 92020

SEARCH WARRANT
CASE NUMBER: ~~SD08PE08SD0015~~
'08 MJ 0844

TO: Special Agent Andrew Soule, Immigration and Customs Enforcement and any Authorized Officer of the United States

Affidavit(s) having been made before me by Special Agent Andrew Soule, Immigration and Customs Enforcement who has reason to believe that __ on the person of or X on the premises known as (name, description and/or location)

See ATTACHMENT A

in the SOUTHERN District of CALIFORNIA there is now concealed a certain person or property, namely (describe the person or property)

See ATTACHMENT B

which is evidence of possible violation of Title 18, United States Code, Sections 473, and 545. I am satisfied that the affidavit(s) and any recorded testimony establish probable cause to believe that the person or property so described is now concealed on the person or premises above-described and establish grounds for the issuance of this warrant.

YOU ARE HEREBY COMMANDED to search on or before March 27, 2008.

As this is an anticipatory search warrant, it will not be executed unless the following conditions precedent occur: Any adult person at the residence of 1097 Emerald Avenue, El Cajon, California 92020, must sign for and accept delivery of the package containing the 20 USD$100 bills addressed from Randolph Kingsley, #15 Alololw Way, Lagos, Nigeria to Randolph Leighton at 1097 Emerald Avenue, El Cajon, California 92020.

(not to exceed 10 days) the person or place named above for the person or property specified, serving this warrant and making the search at any time between 6AM and 10PM in the day or night as I find reasonable cause has been established and if the person or property be found there to seize same, leaving a copy of this warrant and receipt for the person or property taken, and prepare a written inventory of the person or property seized and promptly return this warrant to
as required by law. MAR 17 2008 1:35pm

Date and Time Issued — At SAN DIEGO, CALIF.
City and State

United States Magistrate Judge LEO S. PAPAS (Signature of Judicial Officer)

AO 93 (Rev. 5/85) Search Warrant

RETURN

DATE WARRANT RECEIVED	DATE AND TIME WARRANT EXECUTED	COPY OF WARRANT AND RECEIPT FOR ITEMS LEFT WITH
March 17, 2008	10:05 hours, March 18, 2008	Randolph Lee LEIGHTON

INVENTORY MADE IN THE PRESENCE OF
Elisabeth Cervantes, Special Agent, Immigration & Customs Enforcement

INVENTORY OF PERSON OR PROPERTY TAKEN PURSUANT TO THE WARRANT

See Property Inventory Attachment...

CERTIFICATION

I swear that this inventory is a true and detailed account of the person or property taken by me on the warrant.

3/27/2008

Andrew Soule, Special Agent Immigration & Customs Enforcement — Date

Subscribed, sworn to, and returned before me this date.

3/27/08

United States Magistrate Judge Leo S. Papas — Date

Property Inventory Attachment:

- 20 One hundred dollar bills, counterfeit U.S. currency
- 1 TNT (express mail)envelope
- 5 Computer towers
- 1 Laptop computer
- 19 Loose computer hard drives
- 2 Bags of documents
- 1 12gauge shotgun
- 3 Boxes of 12gauge shotgun ammunition
- 20 Grams of marijuana
- 3 pieces of drug paraphernalia

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

FILED
'08 MAR 17 PM 3:03
CLERK, U.S. DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA
BY: DEPUTY

In the Matter of the Search of
(Name, address or brief description of person or property to be searched)

APPLICATION AND AFFIDAVIT

FOR SEARCH WARRANT

1097 Emerald Ave,
El Cajon, California 92020

CASE NUMBER: ~~SD08PE08SD0015~~ '08 MJ 0844

I Andrew Soule being duly sworn depose and say:

I am a(n) Special Agent, Immigration and Customs Enforcement and have reason to believe that ____ on the person of or X on the premises known as (name, description and/or location)

See ATTACHMENT A

in the SOUTHERN District of CALIFORNIA there is now concealed a certain person or property, namely (describe the person or property)

See ATTACHMENT B

which is (state one or more bases for search and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)

Evidence of the commission of a criminal offense

Concerning a violation of Title 18 United States Code, Section(s) 473 and 545

The facts to support a find of Probable Cause are as follows:

As this is an anticipatory search warrant, it will not be executed unless the following conditions precedent occur: Any adult person at the residence of 1097 Emerald Avenue, El Cajon, California 92020, must sign for and accept delivery of the package containing the 20 USD$100 bills addressed from Randolph Kingsley, #15 Alololw Way, Lagos, Nigeria to Randolph Leighton at 1097 Emerald Avenue, El Cajon, California 92020.

Continued on the attached sheet and made a part thereof. X Yes ~~No~~

Signature of Affiant

Sworn to before me, and subscribed in my presence

as required by law.

MAR 17 2008 1:35 pm at SAN DIEGO, CALIF.

Date and Time Issued City and State

United States Magistrate Judge Leo S. Papas

Signature of Judicial Officer

AFFIDAVIT

I, Andrew Soule, Special Agent for the United States Immigration and Customs Enforcement having been duly sworn, depose and say:

1. I am a Special Agent (SA) of Immigration and Customs Enforcement and has been so employed for approximately 1½ years. My current assignment is Commercial Fraud Investigations. My education and experience includes four years as a U.S. Customs Inspector and Customs and Border Protection (CBP) Officer. During my law enforcement career I have made or participated in hundreds of arrests relating to drug smuggling, alien smuggling and commercial fraud. I received a Bachelor's Degree from San Diego State University and a Master's Degree from National University. I attended the 11 week U.S. Customs Inspections Academy at the Federal Law Enforcement Training Center (FLETC) at Glynco, Georgia. I also attended the 12 week FLETC Criminal Investigator Training Program. Additionally, I attended the 12 week Immigration and Customs Enforcement Special Agent Training Program at the Federal Law Enforcement Training Center at Glynco, Georgia. The information contained in this affidavit is based upon my personal observations, knowledge and discussions with other agents and employees of Immigration and Customs Enforcement, Customs and Border Protection and the Secret Service, as well as the review of documents and other evidence obtained in the course of this investigation.

2. In my experience and the experience of other law enforcement officers including U.S. Secret Service Special Agents with whom I have worked, it is common knowledge that all of the victims and suspects of Nigerian fraud scams are always contacted via the internet. This is usually done with a mass e-mail or by offering to pay excessively high prices on products sold

online. In all cases the victim or suspect responds by providing their contact information, (i.e. name, address, e-mail).

3. It has also been my experience that evidence of such violations of counterfeit obligations or securities, in violation of Title 18, United States Code, Section 473 and Smuggling/Importation contrary to law, Title 18, United States Code, Section 545. Section 473 of Title 18 of the United States Code States that whoever buys, sells, exchanges, transfers, receives or delivers any counterfeited or altered obligation or other security of the United States, with the intent that the same be passed, published or used as true and genuine, shall be fined under this title or imprisoned not more than twenty years, or both. Section 545 of Title 18 of the United States Code that whoever fraudulently or knowingly imports or brings into the United States and merchandise contrary to law shall be fined under this title or imprisoned not more than twenty years, or both.

4. This affidavit is submitted in support of an application for the issuance of an anticipatory search warrant for the residence of Randolph Lee Leighton to search for and seize all items described in Attachment A.

5. The residence of Randolph Lee Leighton is located at 1097 Emerald Avenue El Cajon, California 92020. I know that Leighton currently resides at that residence because a mint green colored 1992 Honda Civic with California license plate 3BKP755, registered to Leighton, has been seen in the driveway of this residence. It is Leighton's current address as listed by the California Department of Motor Vehicles. A Law Enforcement search of the Accurint database listed Leighton as living at the above address from 1993 to present. A physical description pertaining to the residence of Randolph Lee Leighton is further described in Attachment B.

//

//

//

STATEMENT OF PROBABLE CAUSE

6. On March 12th 2008, Customs and Border Protection (CBP) Officer J. Chan conducted a border search examination on a document with House Airway Bill (HAWB) 222273275 that originated from Nigeria. This document arrived on British Airways flight (BA) 283, from London Heathrow airport and flew non-stop to the Los Angeles International Airport, and was then transported to the TNT freight forwarder commercial facility in Los Angeles, California to be forwarded to DHL for delivery within the United States.

CBP Officer J. Chan discovered the package as part of CBP Wing Clip Operations which examines all documents arrived from high risk countries at express consignment facilities. The Shipment was arriving from Nigeria, a high risk country. The shipment was not manifested in the Customs cargo computer for manifest review. The consignee and shipper was an individual person. Chan discovered two other packages that were counterfeit currency seizures both of which originated from Nigeria were accepted for controlled delivery. The document with HAWB 222273275 was un-manifested and was consigned to Randolph Leighton at 1097 Emerald Ave, El Cajon, CA 92020 to be delivered by DHL. The shipper of the parcel is listed as Randolph Kingsley, #15 Alololw Way, Lagos, Nigeria.

7. Upon examination of the document, twenty USD$100 notes totaling USD$2,000.00 were discovered inside the document bearing HAWB 222273275. The counterfeit currency was wrapped with carbon paper. CBP Officer Chan placed the notes under a fluorescent light source but could not see the red and pink security threads, and the watermark. The locations of the security threads should be between the Federal Reserve note and the picture, and the watermark should be on the right side of the note. CBP Chan contacted ICE SA Mattison concerning the

currency. SA Mattison then contacted SA Jay Huang of the United States Secret Service. SA Huang verified that the bills were not genuine.

8. Based upon his inspection and SA Huang's verification CBP Officer Chan determined the twenty U.S. currency notes were counterfeit and seized them. SA Mattison then contacted San Diego ICE SA Andrew Soule who accepted the case.

9. On March 13, 2008 ICE SA Borrero transported the document and counterfeit currency to San Diego where San Diego Ice agents took custody of the document and contents for a controlled delivery to the consignee, Randolph Leighton.

10. On March 13, 2008, ICE SA Yates contacted SA Rick Metzger of the United States Secret Service. SA Metzger is responsible for investigating violations of Title 18 U.S.C. Section 471, 472, 473 and 474, manufacturing, possession, passing and dealing in counterfeit currency or digital and/or electronic images. SA Metzger examined the images of the counterfeit currency supplied by SA Soule and concluded that they were counterfeit varieties of the same bill with variations in the serial number. SA Metzger stated that these types are commonly shipped from Nigeria in a fraud scheme to have real money wired back to Nigeria. SA Metzger stated that usually the recipient of these bills has been contacted via the Internet or by e-mail. The recipients will then communicate either by Internet, e-mail, telephone or mail with the suspect in Nigeria. The suspect in Nigeria will send a parcel containing the counterfeit bills to the recipient. The recipient of the bills will then deposit the counterfeit money and wire a lesser amount to the suspect in Nigeria.

11. On March 13, 2008, SA Yates conducted a check of California Department of Motor Vehicles (DMV) computerized records check on Randolph Leighton. DMV records listed Randolph Lee Leighton as a male with blond hair, blue eyes, 5 feet 11 inches tall, 225 pounds,

with a date of birth of August 03, 1959, residing at 1097 Emerald Dr, El Cajon, CA 92020. Additional Law Enforcement checks in Accurint confirm Randolph Leighton as the resident of 1097 Emerald Dr, El Cajon, CA 92020.

12. On March 13, 2008 ICE SA Chaidez conducted surveillance of the residence located at 1097 Emerald Dr, El Cajon, CA 92020. SA Chaidez visually observed a mint green 1992 Honda Civic bearing California license plate 3BKP755 parked in the driveway of the residence. SA Chaidez queried the license number in the National Law enforcement Telecommunications System (NLETS). NLETS records show that California license 3BKP755 is a 1992 Honda registered to Randolph Lee Leighton of 1097 Emerald Ave, El Cajon, CA 92020.

13. Once the parcel, a DHL package bearing HAWB 222273275 is physically received at the aforementioned premises at 1097 Emerald Ave, El Cajon, CA 92020, probable cause will exist to believe that evidence of a violation of 18 U.S.C. Sections 545, (smuggling goods into the United States), and 18 U.S.C 473, (dealing in counterfeit obligations or securities), of law will be located in that specific location.

17. It is my experience and the experience of law enforcement officers with whom I work that in every case in the past year, subjects reported that the Nigerian money scams were initiated using the internet. They are contacted via mass e-mails or by offering to pay excessive amounts of money for items being sold on the internet. The computer retains the record of the e-mail that facilitates the crime.

Background on Computers

18. The term "computer" as used here is defined as 18 U.S.C. § 1030(e)(1), and includes electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such a device. As

an ICE agent assigned to the Cybercrimes Division, I have had training in the investigation of computer-related crimes. Based upon my experience and knowledge, I know there are several reasons why a complete search and seizure of information from computers often requires seizure of all electronic storage devices, as well as all related peripherals, to permit a thorough search later by qualified computer forensic agents or experts in a laboratory or other controlled environment:

A. Computer storage devices, such as hard disks, diskettes, tapes, laser disks, compact discs, and DVDs, can store the equivalent of hundreds of thousands of pages of information. Additionally, when an individual seeks to conceal information that may constitute criminal evidence, that individual may store the information in random order with deceptive file names. As a result, it may be necessary for law enforcement authorities performing a search to examine all the stored data to determine which particular files are evidence or instrumentalities of criminal activity. This review and sorting process can take weeks or months, depending on the volume of data stored, and would be impossible to attempt during a search on site; and

B. Searching computer systems for criminal evidence is a highly technical process, requiring specialized skill and a properly controlled environment. The vast array of computer hardware and software available requires even those who are computer experts to specialize in some systems and applications. It is difficult to know before a search what type of hardware and software are present and therefore which experts will be required to analyze the subject system and its data. In any event, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources and from destructive code imbedded in the system as a booby trap), a controlled environment is essential to its complete and accurate analysis.

19. Based on my own experience and my consultation with other agents who have been involved in computer searches, searching computerized information for evidence or instrumentalities of a crime often requires the seizure of all of a computer system's input and output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

A. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices; and

B. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit (CPU). In cases like the instant one where the evidence consists partly of image files, the monitor and printer are also essential to show the nature and quality of the graphic images which the system could produce. Further, the analyst again needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

C. I am familiar with and understand the implications of the Privacy Protection Act ("PPA"), 42 U.S.C. § 2000aa, and the role of this statute in protecting First Amendment activities. I am not aware that any of the materials to be searched and seized from the SUBJECT PREMISES are protected materials pursuant to the PPA. If any such protected materials are inadvertently seized, all efforts will be made to return these materials to their authors as quickly as possible.

Computer Search Protocol

20. With the approval of the court in signing this warrant, agents executing this search warrant will employ the following procedures regarding computers that may be found at the premises which many contain information subject to seizure pursuant to this warrant:

A. There is probable cause to believe that the computer used to receive and send communications involving money scams originating in Nigeria described herein constitute "property used in committing a crime" with the meaning of Rule 41(c)(3), Federal Rules of Criminal Procedure. Consequently, such computer(s) are subject to seizure. In addition, images or data of. The computer equipment, digital storage media, modems, keyboards, monitors and any peripherals discovered during the search will be seized and transported offsite for imaging and if such equipment contains images or data of communications involving money scams originating in Nigeria will be retained as instrumentalities and evidence of criminal activity. The digital media will be imaged for analysis, but the computer equipment will not be returned. Should the owner of the computer seek the return of any legal computer files or documents, the owner shall make such a request in writing to the U.S. Attorney's Office and shall include the names of specific file and/or documents sought. The U.S. Attorney's Office shall forward such written request to ICE and every attempt will be made to capture and return only the files and/or documents requested within 60 days of the written request. If no images or data of communications involving money scams originating in Nigeria are found on any of the seized equipment, the equipment will be returned within 60 days.

B. A forensic image is an exact physical copy of the hard drive or other media. It is essential that a forensic image be obtained prior to conducting any search of the data for information subject to seizure pursuant to this warrant. A forensic image captures all of the data on the hard drive or other media without the data being viewed and without changing the data in anyway. This is in sharp contrast to what transpires when a computer running the common Windows operating system is started, if only to peruse and copy data - data is irretrievably changed and lost. Here is why: When a Windows computer is started, the operating system proceeds to write hundreds of new files about its status and operating environment. These new files may be written to places on the hard drive that may contain deleted or other remnant data. That data, if overwritten, is lost permanently. In addition, every time a file is accesses, unless the access is done by trained professionals using special equipment, methods and software, the operating system will re-write the metadata for that file. Metadata is information about a file that the computer uses to manage information. If an agent merely opens a file to look at it, Windows will overwrite the metadata which previously reflected the last time the file was accessed. The lost information may be critical.

C. Special software, methodology and equipment is used to obtained forensic images. Among other things, forensic images normally are "hashed", that is, subjected to a mathematical algorithm to the granularity of 10^{38} power, an incredibly large number much more accurate than the best DNA testing available today. The resulting number, known as a "hash value" confirms that the forensic image is an exact copy of the original and also serves to protect the integrity of the image in perpetuity. Any change, no matter how small, to the forensic image will affect the hash value so that the image can no longer be verified as a true copy.

D. Forensic Analysis: After obtaining a forensic image, the data will be analyzed. Analysis of the data following the creation of the forensic image is a highly technical process that requires thousands of different hardware items and software programs that can be commercially purchased, installed and custom-configured on a user's computer system. Computers are usually customized by their users. Even apparently identical computers in an office environment can be significantly different with respect to configuration, including permissions and access rights, passwords, data storage and security. It is not unusual for a computer forensic examiner to have to obtain specialized hardware or software, and train with it, in order to view and analyze imaged data.

E. Analyzing the contents of a computer, in addition to requiring special technical skills, equipment and software also can be very tedious. It can take days to properly search a single hard drive for specific data. Searching by keywords, for example, often yields many thousands of "hits," each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant "hit" does not end the review process. As mentioned above, the computer may have stored information about the data at issue: who created it, when it was created, when it was last accessed, when was it last modified, when was it last printed and when it was deleted. Sometimes it is possible to recover an entire document that was never saved to the hard drive if the document was printed. Operation of the computer by non-forensic technicians effectively destroys this and other trace evidence. Moreover, certain file formats do not lend themselves to keyword searches. Keywords search text. Many common electronic mail, database and spreadsheet applications do not store data as searchable text. The data is saved in a proprietary non-text format. Microsoft Outlook data is an example of a commonly used program which stores data in non-textual, proprietary manner-ordinary keyword searches will not reach this data. Documents printed by the computer even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. Similarly, faxes sent to the computer are stored as graphic images and not as text.

F. Analyzing data on-site has become increasingly impossible as the volume of data stored on a typical computer system has become mind-boggling. For example, a single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double spaced pages of text. Computer hard drives are now capable of storing more than 100 gigabytes of data and are commonplace in new desktop computers. And, this data may be stored in a variety of formats or encrypted. The sheer volume of data also has extended the time that it takes to analyze data in a laboratory. Running keyword searches takes longer and results in more hits that must be individually examined for relevance. Even pursuing only a directory listing of a home computer can result in thousands of pages of printed material most of which likely will be limited probative value.

G. Based on the foregoing, searching any computer or forensic image for the information subject to seizure pursuant to this warrant may require a range of data analysis techniques and may take weeks or even months. Keywords need to be modified continuously based upon the results obtained; criminals can mislabel and hide files and directories, use codes to avoid using keywords, encrypt files, deliberately misspell certain words, delete files and take other steps to defeat law enforcement. In light of these difficulties, I request permission to use whatever data analysis techniques reasonably appear necessary to locate and retrieve digital evidence within the scope of this warrant.

H. All forensic analysis of the imaged data will be directed exclusively to the identification and seizure of information with the scope of this warrant. In the course of proper examination, the forensic examiner may view information not within the scope of the warrant. Such information will not be made available to the investigating agents unless it appears to the examiner that the information relates to the commission of offenses not covered by this warrant. In that event, the examiner will confer wit the investigator so that the investigator can determine whether to seek a further search warrant for newly uncovered data.

21. In conclusion, based upon the information contained in this affidavit, I believe there is probable cause to support the issuance of a search warrant for the residence located at 1097 Emerald Avenue, El Cajon, CA 92020, more particularly described in Attachment "A", and furthermore that there is probable cause that these premises contain evidence of violations of 18 U.S.C. Sections 545, (smuggling goods into the United States), and 18 U.S.C 473, (dealing in counterfeit obligations or securities).

22. As this is an anticipatory search warrant, it will not be executed unless the following conditions precedent occur: Any adult person at the residence of 1097 Emerald Avenue, El Cajon, California 92020, must sign for and accept delivery of the package containing the 20

USD$100 bills addressed from Randolph Kingsley, #15 Alololw Way, Lagos, Nigeria to Randolph Leighton at 1097 Emerald Avenue, El Cajon, California 92020

Request for Sealing

23. It is further respectfully requested that this Court issue an Order sealing, until further order of this Court, all papers submitted in support of this Application, including the Application, Affidavit, and Search Warrant, and the requisite inventory notice. Sealing is necessary because the items and information to be seized are relevant to an ongoing investigation and premature disclosure of the contents of this affidavit and related documents may have a negative impact on this continuing investigation and may jeopardize its effectiveness.

Further affiant sayeth not.

I declare under penalty and perjury that the foregoing is true and correct to the best of my knowledge.

Andrew Soule
Special Agent,
U.S. Immigration and Customs Enforcement

SWORN AND SUBCRIBED TO before me this 17 day of March 2008.

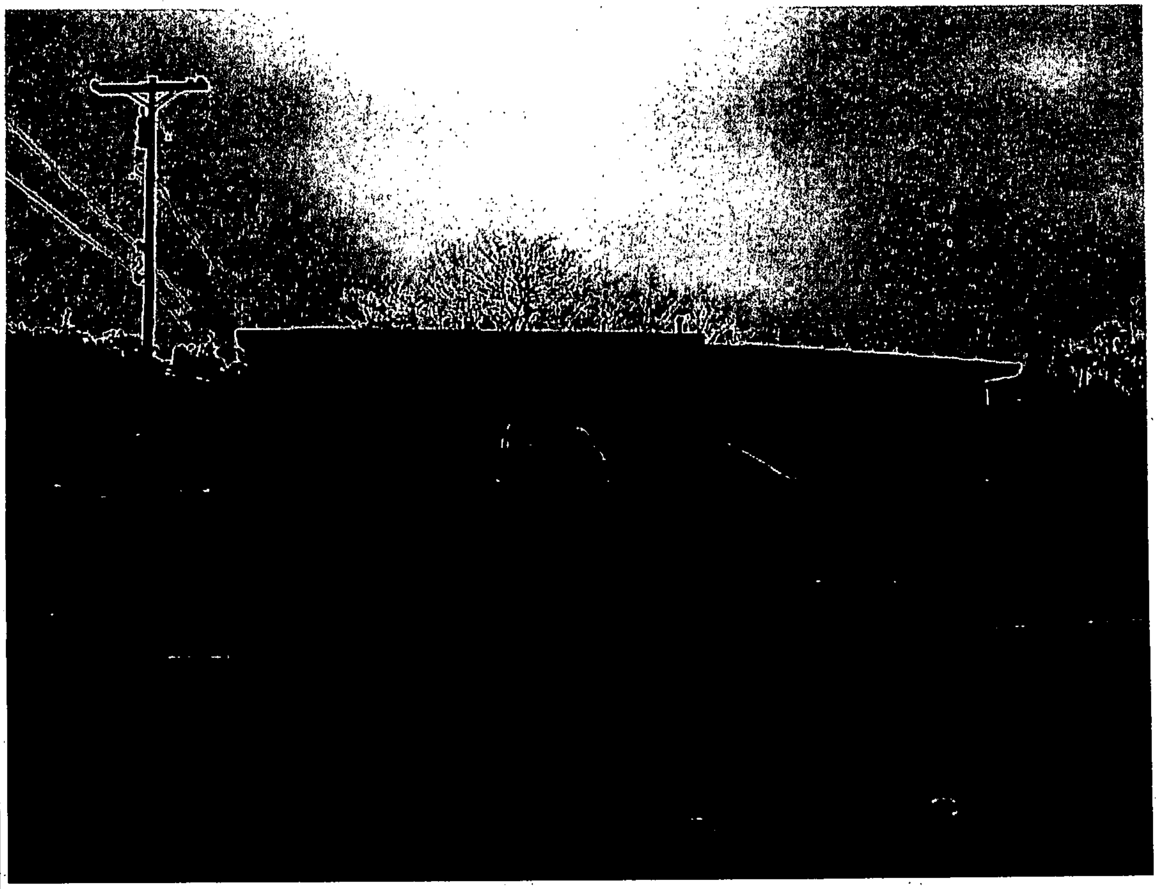
LEO S. PAPAS
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF THE PREMISES TO BE SEARCHED

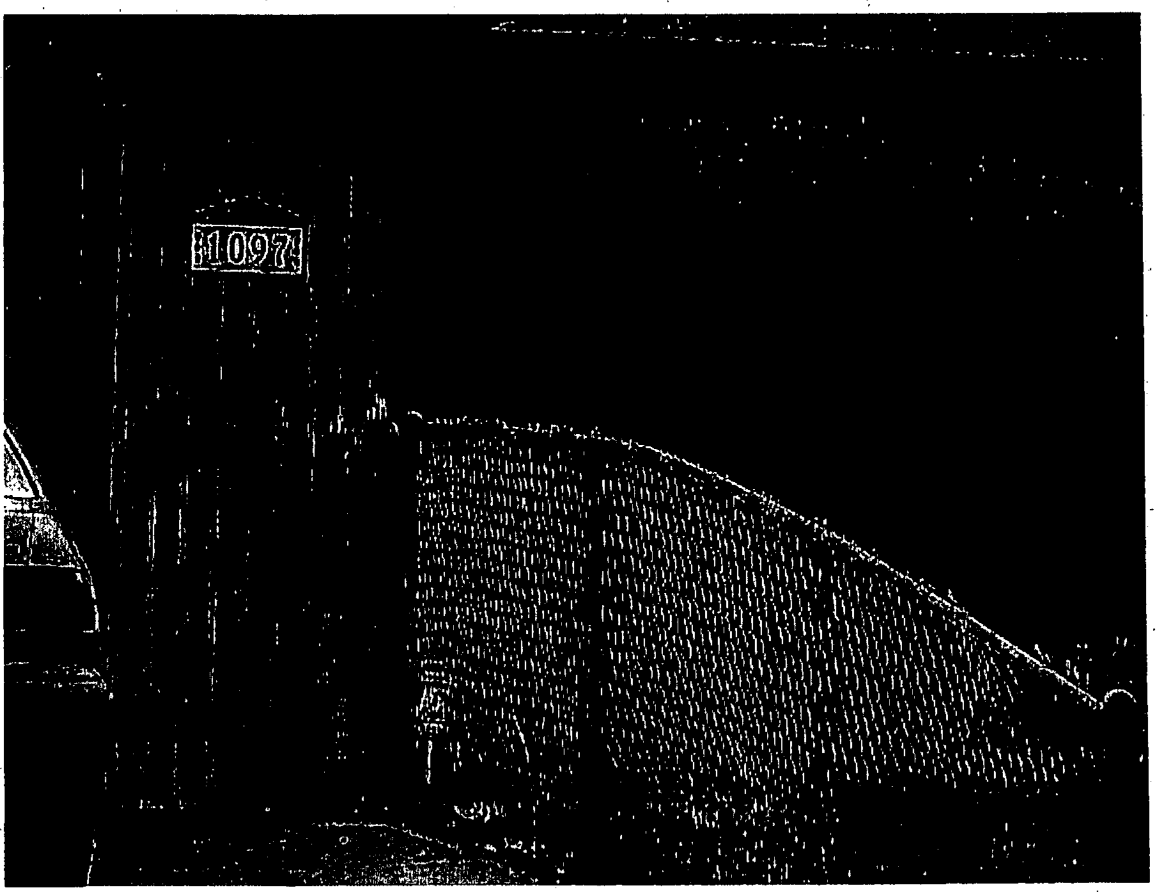
This affidavit is submitted in support of a search warrant for one (1) single family residence described as follows:

A single-family dwelling located at 1097 Emerald Ave, El Cajon, CA 92020, more fully described as: A tan colored, wooden exterior, single story residence with brown trim and a grey roof. The residence has a white colored two-car garage door and a brown colored metal security front door. The residence is located on the corner of West Chase Avenue and Emerald Avenue. The residence faces Emerald Avenue with the address of 1097 clearly displayed on the right side of the garage door above a gold colored mail slot. The address is displayed on green metal frame with a white background and black numeric characters. The residence is further described as having a four-foot chain link fence around the front and side yard, which faces West Chase Avenue.



1097 Emerald Ave. El Cajon, CA 92020.

West side of the house viewed from Emerald Ave.



1097 Emerald Ave. El Cajon, CA 92020.

Close-up photo of address marker on the house

ATTACHMENT B

PROPERTY TO BE SEIZED

a) DHL Parcel Tracking No. HAWB 222273275 and its contents which are addressed to Randolph Leighton at 1097 Emerald Ave, El Cajon, CA 92020 and having a return address as being sent from Randolph Kingsley, #15 Alololw Way, Lagos, Nigeria.

b) Any and all counterfeit U.S. currency;

c) Any and all storage containers used to store counterfeit U.S. currency;

d) All records relating the counterfeiting of U.S. currency, including (but not limited to) images or partial images of U.S. currency, lists of customers and related identifying information; types, amounts, and prices of counterfeit currency printed as well as dates, places, and amounts of counterfeit passed; any information related to sources of counterfeit paraphernalia (including names, addresses, phone numbers, or any other identifying information);

e) Any mail, correspondence, documents, packing materials, letters from Nigeria.

f) COMPUTERS, COMPUTER EQUIPMENT, AND COMPUTER RECORDS — The terms records, documents, programs, application or materials includes records, documents, programs, applications or materials created, modified or stored in any capacity.

In searching for data capable of being read, stored or interpreted by a computer, law enforcement personnel executing this search warrant will employ the following procedure:

(1) Upon securing the premises, law enforcement personnel trained in searching and seizing computer data (the "computer personnel") will make an initial review of any computer equipment and storage devices to determine whether it is

practical to perform an on-site search or make an on-site copy of the data during the execution of the search in a reasonable amount of time without jeopardizing the ability to preserve the data. Any copy made by the computer personnel will be a forensic image of the computer's entire storage devices. The forensic image will be transported to an appropriate law enforcement laboratory. The computer personnel will then review the forensic image in order to extract and seize any data that falls within the list of items to be seized set forth herein. The Government will retain all forensic images made of the computer's storage devices. Law enforcement personnel will make all reasonable efforts to perform an on-site search or make an on site-copy of the data within a reasonable amount of time.

(2) If the computer personnel determine it is not practical to perform an on-site search or make an on-site copy of the data within a reasonable amount of time, then the computer equipment and storage devices will be seized and transported to an appropriate law enforcement laboratory for review. The computer equipment and storage devices will be reviewed by appropriately trained personnel in order to extract and seize any data that falls within the list of items to be seized set forth herein. In order to extract and seize data that falls within the list of items to be seized, the computer personnel will first make a forensic image of the computer's storage devices. The computer personnel will then review the forensic image in order to extract and seize any data that falls within the list of items to be seized set forth herein. After inspecting and imaging the seized computer equipment and storage devices the computer equipment will not be returned. Should the owner of the computer seek the return of any legal computer files or documents, the owner shall make such a request in writing to the U.S. Attorney's Office and shall include the names of specific file and/or documents sought. The U.S. Attorney's Office shall forward such written request to ICE

and every attempt will be made to capture and return only the files and/or documents requested within 60 days of the written request. If no images or data of communications involving money scams originating in Nigeria are found on any of the seized equipment, the equipment will be returned within 60 days.

(3) In searching the data, the computer personnel may examine all the data contained in the computer equipment and storage devices to view their precise contents and determine whether the data fall within the items to be seized as set forth herein. In addition, the computer personnel may search for and attempt to recover "deleted," "hidden," or encrypted data to determine whether the data falls within the list of items to be seized as set forth herein.

In order to search for data that is capable of being read or interpreted by a compute, law enforcement will need to seize and search the following items, subject to the procedures set forth above:

(1) Any computer equipment and storage device capable of being used to commit, further or store evidence of the offense listed above:

(2) Any computer equipment used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners;

(3) Any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CE-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, and personal digital assistants;

(4) Any documentation, operating logs and reference manuals regarding the operation of the computer equipment, storage devices or software;

(5) Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices or data to be searched;

(6) Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

(7) Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

ANDRE